Initiate a 24/7 Security Monitoring Center and Improve Threat Hunting Capabilities

FY2022 Request: **$1,700,000**
Reference No: **63848**

AP/AL: Appropriation

Project Type: Information Technology / Systems / Communication

Category: General Government

Location: Statewide

House District: Statewide (HD 1-40)

Impact House District: Statewide (HD 1-40)

Contact: Leslie Isaacs

Estimated Project Dates: 07/01/2021 - 06/30/2026

Contact Phone: (907)465-5655

Brief Summary and Statement of Need:

Establish enhanced statewide security operations center (SOC) function with managed defense capabilities for a period no more than 24 months. This project will strengthen detection and response to cybersecurity threats in the short term while the State Security Office (SSO) plans and implements long term SOC capabilities.

Funding:	FY2022	FY2023	FY2024	FY2025	FY2026	FY2027	Total
1004 Gen Fund	$1,700,000						$1,700,000
Total:	$1,700,000	$0	$0	$0	$0	$0	$1,700,000

☐ State Match Required ☐ One-Time Project ☐ Phased - new ☑ Phased - underway ☐ Ongoing
0% = Minimum State Match % Required ☐ Amendment ☐ Mental Health Bill

Operating & Maintenance Costs:

	Amount	Staff
Project Development:	0	0
Ongoing Operating:	0	0
One-Time Startup:	0	
Totals:	0	0

Prior Funding History / Additional Information:

Project Description/Justification:

The State of Alaska has experienced several security incidents over the past 12 months and continues to block thousands of intrusion attempts each month. These intrusion attempts put a strain on our limited staffing in the State Security Office and Office of Information Technology (OIT). As an example, most recently the critical Log4j vulnerability consumed1,315 hours of staff time (7 employees, including after-hours work time) during a 3-week period to remediate over 1,000 vulnerable systems. To best protect Alaskan citizen's data, the State of Alaska needs to expand its capability to identify potential threats in real-time and mitigate them before any loss of personally identifiable information (PII), protected health information (PHI) interruptions to state delivered services occur.

This funding will establish 24/7 managed Security Operations Center (SOC) coverage for up to 24 months and provide the SSO ability to further explore SOC options. It will also determine enduring requirements and the best path forward to complete the following: implement internal and external capabilities, strengthen detection and response to cybersecurity threats, improve SOC processes and procedures, identify and secure high risk vulnerabilities, and ascertain the true cost of SOC

provided services.

Cybercriminals and Nation State Actors work around the clock attempting to exploit our defenses. The State of Alaska cannot afford delays in detection or response when staff go home or are consumed by other cybersecurity matters (such as Log4j). An SOC delivers non-stop monitoring and immediate threat hunting protection against security threats. Sustainability of a 24/7 SOC presents numerous challenges, however the State can subscribe to SOC-as-a-service and benefit from security monitoring services while planning a sustainable path forward. The 'as a service' consumption model will provide cost stability and operational expediency.

Line Item Allocation:

Line Item	Amount
1000 Personal Services	
2000 Travel	
3000 Services	$1,700,000
4000 Commodities	
5000 Capital Outlay	
7000 Grants	
TOTAL	$1,700,000